Предмет комплексной системы защиты информации в организации

Обеспечение национальных интересов страны тесно связано с деятельностью коммерческие организации, имеющих доминирующее положение в рыночной экономике. Доктрина информационной безопасности Российской Федерации отдельно не выделяет угрозы интересам организаций и меры по их предупреждению, а формулирует лишь общие положения по обеспечению информационной безопасности (ИБ) интересов личности, общества и государства. Поэтому организации с учетом особенностей своей деятельности вынуждены формировать собственную систему обеспечения безопасности, используя для этой цели нормы действующего законодательства, и прежде всего в ФЗ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне», а также возможности, трудового корпоративного и гражданско-правового регулирования.

Предметом учебного курса является правовое регулирование порядка установления режима коммерческой тайны и его обеспечение в процессе производства и реализации товаров, выполнения работ и оказания услуг; формирование и развитие комплексной системы защиты информации в организациях.

Для уяснения *предмета комплексной системы защиты информации в организации* необходимо обратиться к понятию деятельности, связанной с функционированием такой системы.

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646)
2. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (в ред. от 18 апреля 2018 г.)

В литературе содержатся различные подходы к регулированию комплексной системы обеспечения безопасности организаций. Большинство авторов при определении понятия такой системы справедливо включают в нее три взаимосвязанных элемента: «интересы — угрозы — защита», отмечая при этом их основополагающую роль в непрерывном процессе обеспечения безопасности любого объекта общества и государства. Безусловно, этот вывод имеет прямое отношение к построению системы обеспечения ИБ организаций, но требует уточнения применительно к механизму безопасности организации.

Под *интересами* в данном случае понимаются частные интересы организаций и индивидуальных предпринимателей, динамично связанные с их экономическими (коммерческими) целями и задачами

Угрозы (внутренние и внешние) обычно выражаются в негативных проявлениях, реально или потенциально препятствующих организации по достижению своих частных целей и создающих опасность ее жизненно важным интересам

Под *защитой информации* в данном случае имеются в виду меры организационного, правового и научно-методического характера, реализация которых позволяет защищать *коммерчески значимую информацию* (КЗИ) от непреднамеренного воздействия, несанкционированного доступа, от разглашения и утечки информации, включая деятельность по предотвращению получения информации конкурентной разведкой с целью обеспечения стабильного и устойчивого экономического развития организации.

Деятельность по обеспечению охраны конфиденциальности информации в гражданском (торговом) обороте может быть представлена в виде совокупности продолжающихся в течение длительного времени действий, направленных на увеличение доходов организации, исключение неоправданных расходов, сохранение положения на рынке производства и реализации товаров или получение иной коммерческой выгоды. Постоянный характер этих действий можно объяснить тем, что информация, обращаемая в организациях, овеществляется во всех факторах общественного производства и составляет начальный, «нулевой» цикл по отношению к любому производимому товару, выполняемой работе и оказываемой услуге.

Субъектами такого рода деятельности выступают лица, относимые доктриной коммерческого права к различным видам субъектов коммерческого права . Они реализуют свои коммерческие цели в условиях оборотоспособности товаров, являющихся объектами торгового права, а также гражданского права. Деятельность по обеспечению охраны коммерческой тайны заключается в оказании помощи хозяйствующим субъектам в решении стоящих перед ними задач.

Обеспечение как средство деятельности, т.е. «то, чем обеспечивают кого-нибудь или что-нибудь», представляет собой совокупность материальных, финансовых, правовых, организационных, технических и иных средств, которые повышают эффективность деятельности организации по достижению своих целей.

При определении *целей обеспечения информационной безопасности организации* следует учитывать, что коммерческая организация представляет собой сложную информационную систему. Это объясняется тем, что конкуренция обусловливает обновление ассортимента и улучшение качества выпускаемых товаров, достижение которых возможно за счет введения в рыночный оборот новой технической, технологической и деловой информации. В этой связи КЗИ постоянно подвергается различным внутренним и внешним угрозам со стороны конкурентов и других лиц. Меры по обеспечению ИБ организаций направлены на исключение фактов разглашения (утечки) КЗИ и несанкционированного доступа к ней. Реализация мер должна обеспечивать не только собственно безопасность статуса КЗИ, но и способствовать стабильному развитию организации, увеличению ее доходов и получению иной коммерческой выгоды.

Целями обеспечения информационной безопасности организаций является защита их законных прав во взаимоотношениях с органами государственной власти и местного самоуправления, партнерами и конкурентами, поддержание внутреннего порядка управления, повышения конкурентоспособности производимых товаров, развитие кооперированных связей и недопущение зависимости от недобросовестных конкурентов и партнеров, ориентация развития техники и технологий на мировые стандарты по профилю деятельности организации, создание благоприятной рыночной конъюнктуры и рост прибылей за счет эффективного использования *коммерчески значимой информации* в рекламе. Достижение указанных целей требует решения ряда *задач* по своевременному выявлению угроз жизненно важным интересам, оперативному использованию правовых средств предупреждения причин и обстоятельств, способствующих правонарушениям и ведущим к открытию возможных каналов утечки (ВКУ) *коммерчески значимой информации*, пресечению неправомерных действий лиц и возмещению убытков.

Реализация задач требует от организаций соблюдения принципов законности при осуществлении мер информационной безопасности с учетом разрешенных законом методов выявления, предупреждения и пресечения правонарушений в сфере обращения *коммерчески значимой информации*; экономической целесообразности мероприятий по обеспечению информационной безопасности которые не должны снижать экономические показатели деятельности организации и се прибыль; взаимодействия и координации мер по защите *коммерчески значимой информации* с партнерами; профессионализма и ответственности работников, специализирующихся по конкретным направлениям информационной безопасности организаций, их ответственности за результаты своей деятельности.

С понятием и целями обеспечения безопасности тесно соприкасаются — *угрозы информационной безопасности организаций.* Угрозы национальным интересам России, действующие в информационной сфере, оказывают дестабилизирующее влияние на ИБ организаций. В их числе ведущее место занимают *общие угрозы,* направленные на дезорганизацию национальной экономики; экономическую блокаду в форме целенаправленной конкуренции путем вытеснения собственного производства импортом товаров из-за рубе жа; технологическую блокаду, выражающуюся в существенном сокращении финансирования науки и образовании в этой связи негативных тенденций, ведущих к деградации российской экономики до уровня природно-сырьевого анклава мирового хозяйства; криминализацию общества в условиях утраты государством контроля над финансовой деятельностью организаций и др.

Кроме общих угроз, на уровне хозяйственных связей организации в гражданском (торговом) обороте действуют *конкретные угрозы*, которые возникают вследствие *нарушений* работниками режима *коммерчески значимой информации* на каналах возможной ее утечки и контрагентами своих обязательств по охране такой информации. В данном случае под коммерческой тайной понимается режим *коммерчески значимой информации* (п. 1 ст. 3 Закона о коммерческой тайне), имеющий коммерческую значимость. В отношении такой информации вводится режим коммерческой тайны. Поэтому названные в тексте термины употребляются как идентичные, если иное не оговорено специально.

Характеристика нарушений режима *коммерчески значимой информации* включает совокупность признаков: 1) раскрывающих структуру нарушений и иерархии управления по видам производственной и коммерческой деятельности; 2) характеризующих сферы профессиональной деятельности исполнителей, в которых наблюдаются проявления нарушений; 3) отражающих личностные особенности лиц, виновных в совершении нарушений; 4) имеющих значение для понимания причин нарушений режима *коммерчески значимой информации* и осуществления субъектами предупредительной деятельности.

Нарушения режима *коммерчески значимой информации* чаще всего выражаются в невыполнении или ненадлежащем выполнении работниками своих служебных обязанностей и партнерами договорных обязательств. Администрация организаций оперирует существенно суженным представлением о формах проявления нарушений режима *коммерчески значимой информации* ведущих к появлению *возможных каналов утечки* информации. Реагирование порой связывается лишь с нарушениями внутриобъектового и пропускного режима, лежащими «на поверхности» и не требующими больших усилий по их выявлению.

Вместе с тем другие нарушения, которые ведут к разглашению (утечке) *коммерчески значимой информации* не устанавливаются и меры по ним не принимаются. Речь идет о нарушениях на каналах оперативной связи с использованием мобильных телефонов и Интернет, переписки по служебным вопросам, публикации материалов в открытой печати, приема и увольнения работников, работы с командированными лицами, связанными с функционированием допускной и разрешительной системы в организациях.

Выяснение правовой природы названных нарушений требует *учета связи противоречий и причин нарушений режима коммерчески значимой информации* . Общая причина нарушений режима *коммерчески значимой информации* обусловлена существованием противоречий в социально-экономическом развитии страны и с несвоевременным или неправильным их разрешением в рыночных условиях хозяйствования. На основе анализа факторов, способствующих совершению нарушений режима *коммерчески значимой информации*, можно выделить *ряд противоречий, ведущих к дестабилизации положения организации в области обеспечения ее информационной безопасности.*

.Речь идет об отсутствии должного реагирования администрации на происходящие изменения в законодательстве и коммерческой практике, оказывающие влияние на стабильность хозяйственной ситуации, и принятии адекватных мер защиты КЗИ; о нормативных требованиях, предъявляемых к подбору кадров, имеющих доступ к КЗИ, и практикой назначения на должности лиц, не подготовленных к выполнению функциональных обязанностей по охране конфиденциальности информации; о закреплении в корпоративных актах и трудовых договорах функций отдельных категорий работников, профессионально занимающихся защитой КЗИ, и объективными возможностями их надлежащего выполнения в практической деятельности; об установленной нормами законодательства системе реализации ответственности за нарушения в сфере обращения КЗИ и несоблюдении на практике принципа неотвратимости ответственности за совершение нарушений режима КЗИ и др.

Названные противоречия имеют *конкретные причины,* действующие на уровне организаций, которые в свою очередь обусловлены различными *обстоятельствами организационно-управленческого, материально-экономического и правового характера.* Можно говорить о недостатках в организации и управлении процессом обеспечения ИБ, отсутствии должного порядка и договорной дисциплины во взаимоотношениях с партнерами по защите КЗИ;

Установление особенностей *личности правонарушителей* ре жима коммерческой тайны важно для решения комплекса задач в сфере правового обеспечения ИБ организаций. Получение ха рактеристики на них представляет большую сложность с учетом специфики их профессиональной деятельности в сфере обращения КЗИ, взаимодействия личности и ситуаций, возникающих в связи с изменением оперативной обстановки в организации.

Изучение социально-демографических признаков, нравственных свойств и психологических особенностей лиц, совершивших правонарушения в информационной сфере, где обращается КЗИ, показывает, что они тесно взаимосвязаны и взаимообусловлены, обеспечивают целостную характеристику только в их совокупности и могут рассматриваться в качестве информационной модели личности нарушителя режима коммерческой тайны. При проведении воспитательно-профилактической работы следует учитывать, что социально-демографические особенности не являются таковыми, которые указывали на отличия правонарушителей режима коммерческой тайны от законопослушных граждан. У лиц, совершивших такие правонарушения, более деформировано правовое сознание (например, представление о концептуальных положениях правового обеспечения ИБ организации, знание правовых норм в этой сфере и др.). И главное, у них более деформировано сознательное отношение в силу отсутствия необходимых материальных стимулов к соблюдению требований режима коммерческой тайны, чем у законопослушных граждан.

Обеспечение безопасности организаций связано с разработкой и осуществлением организационных, правовых, технических, воспитательных и иных *мер,* направленных на поддержание установленного порядка выполнения конфиденциальных работ и обращения с документами и изделиями, содержащими КЗИ, в целях предотвращения ее разглашения (утечки).

Сложившаяся в организациях система мер, устанавливающая и обеспечивающая режим конфиденциальности КЗИ, получила в теории и на практике название как система «режимных мер». Она включает в себя две основные группы.

Во-первых, это *меры, устанавливающие режим коммерческой тайны* до начала производства и реализации товаров, выполнения работ и оказания услуг.

Во-вторых, это *меры, обеспечивающие безопасность организации* в процессе обращения КЗИ при производстве и реализации товаров (работ, услуг).

В основу данной классификации положен принцип учета разделения деятельности в области охраны конфиденциальности информации, определяющий необходимость первоначального установления режима коммерческой тайны в организации, где обращается КЗИ, а затем режимного обеспечения проводимых конфиденциальных работ с использованием различных правовых и иных средств (ст. 10 Закона о коммерческой тайне). Организация должна заранее предпринять усилия по созданию необходимых материальных и иных условий сохранения в тайне важной для нее информации и тем самым обеспечить закрытие ВКУ КЗИ или нейтрализацию их действия.

В связи с этим *первая группа режимных мер,* по сути, *образует режим конфиденциальности КЗИ,* определяемый в Законе о коммерческой тайне как коммерческая тайна со всеми составляющими его элементами, о которых в общих чертах говорится в ст. 10 данного Закона. Эффективность режимных мер этой группы определяется условиями, широко используемыми на практике и закрепленными в Законе. Меры признаются разумно доста точными в том случае, если исключается доступ к информации любых лиц без согласия обладателя и обеспечивается возможность ее использования работниками и контрагентами без нарушения режима конфиденциальности КЗИ. Установленный режим, с одной стороны, должен гарантировать сохранность коммерческих секретов, а с другой — может ограничивать права работников и взаимоотношения с партнерами по поводу передачи им КЗИ. При выборе режимных мер следует учитывать возможные отрицательные последствия их применения с учетом задач, стоящих перед организацией, и соблюдения принципа законности

По содержанию *первая группа режимных мер* включает *мероприятия подготовительного характера,* направленные на реальное обеспечение защиты КЗИ путем установления соответствующего режима допуска и доступа лиц к такой информации и требующие соответствующего ресурсного обеспечения. К их числу относятся такие мероприятия, как изучение оперативной обстановки организации в целях выявления угроз ее безопасности, определение перечня сведений, составляющих КЗИ, закрепление в корпоративных актах требований к лицам, допускаемым к коммерческим секретам, а также порядка установления, изменения и снятия грифа «Коммерческая тайна», определение порядка учета, хранения и обращения конфиденциальных документов и изделий, содержащих такие сведения, разработку мер организационно-технического характера по противодействию разведывательной деятельности конкурирующих фирм (легендирование, маскировка и зашифровка объекта и работ), осуществление мероприятий, связанных с защитой КЗИ в рамках трудовых и гражданско-правовых отношений, и др.

Вторая группа режимных мер включает мероприятия по выявлению угроз и возможных каналов утечки КЗИ, установлению причин и обстоятельств, способствующих совершению правонарушений в сфере обращения такого рода информации, осуществлению контроля за выполнением требований режима конфиденциальности КЗИ. Содержанием мер данной группы являются *мероприятия обеспечительного характера,* которые включают: 1) формирование методической базы по выявлению правонарушений в сфере обращения КЗИ путем проведения систематического и всестороннего контроля за фактическим состоянием режима конфиденциальности КЗИ на всех стадиях научной, производственной и коммерческой деятельности, воспитательно-профилактической работы в трудовых коллективах с учетом состояния трудовой и договорной дисциплины, моделирования ВКУ КЗИ на основе результатов аналитических и маркетинговых исследований; 2) принятие мер по предупреждению нарушений режима конфиденциальности КЗИ в процессе производства товаров (работ, услуг); 3) пресечение незаконных действий лиц в сфере обращения КЗИ путем передачи материалов о выявленных нарушениях в следственные и административные органы, а также направления исков в суд о возмещении убытков и др.

Направления деятельности по установлению режима коммерческой тайны и обеспечению информационной безопасности:

Во-первых, это установление порядка допуска и доступа лиц к КЗИ и его режимное сопровождение; оформление трудовых соглашений с работниками по поводу охраны коммерческой тайны. Нужно иметь в виду, что порядок допуска лиц к коммерческой тайне законодательно не закреплен. Организации проявляют собственную инициативу по проверке лиц, допускаемых к секретам, что нередко сопровождается грубыми нарушениями конституционных прав и свобод граждан. Что касается порядка доступа лиц к КЗИ, получившего на практике название «разрешительной системы», то он конкретизируется корпоративными актами применительно к условиям деятельности той или иной организации.

Во-вторых, это создание участка (подразделения) для ведения конфиденциального делопроизводства и его материально-техническое обеспечение (оборудование режимных помещений, оснащение ЭВМ, оргтехникой и т.д.).

В-третьих, это обеспечение защиты КЗИ в автоматизированных системах управления производственными и коммерческими процессами. Особенности технологии вычислительных и автоматизированных систем не позволяют в полной мере осуществить перекрытие ВКУ КЗИ. Обеспечение режима на данном направлении работы осуществляется с помощью технических, программных, организационных и иных мер, которые позволяют повысить уровень защиты КЗИ от возможной ее утечки.

В-четвертых, это регулирование внутриобъектового и пропускного режима в организациях, поддержание надежной охраны режимных объектов и изделий в процессе их изготовления и транспортировки. Особенность этого направления состоит в том, что режим конфиденциальности обеспечивается во взаимодействии с органами МВД, транспортными и другими организациями.

В-пятых, это установление гражданско-правовых договорных отношений с отечественными и зарубежными контрагентами по поводу передачи и защиты КЗИ.

Перечисленные направления деятельности составляют предмет правового регулирования *комплексной системы защиты информации в организации.*

2. Методы комплексной системы зашиты информации в организации

В философском смысле слово «метод» — это комплекс интеллектуальных действий, с помощью которых наука предполагает установить истины, к которым она стремится.

Всеобщий философский метод познания используется в познании существа любых явлений, происходящих в сфере обращения КЗИ. Основные категории философии отражают в нашей мысли универсальные законы объективного мира, помогают осмыслить появление новой категории «коммерчески значимая информация» в гражданском и коммерческом праве, в связи с изучением процессов правового регулирования обращения КЗИ и охраной ее конфиденциальности в рыночной экономике.

Для раскрытия комплексного характера системы защиты информации в организации существенное значение имеет изучение таких философских категорий, как часть и целое, система, содержание, структура и форма, внутренняя и внешняя сторона обращения КЗИ (внутренняя и внешняя среда), причины и условия (обстоятельства), возможность, действительность и вероятность, качество, количество и мера и другие категории философии.

Общенаучные методы в силу своей общенаучное непосредственно связаны с всеобщим методом познания и расширяют границы изучения предмета, играют важную роль в соединении философских понятий и категорий с частнонаучными методами правоведения. Преломляясь, образно говоря, через общие философские методы, общенаучные методы оказывают влияние на формирование научной базы частнонаучных методов, позволяющих более конкретно раскрыть закономерности изучаемого объекта. Охарактеризуем те методы, которые имеют непосредственную связь с направлениями формирования и развития комплексной системы защиты информации в организации.

Метод логического подхода. Логика определяется как наука о мышлении, закономерностях в связях и развитии мыслей. Сам процесс правильного логического мышления истолковывается как такая связь мыслей, которая дает возможность прийти к верному выводу в результате рассуждения и делает наши мысли, облеченные в материальную языковую оболочку, понятными и убедительными для других людей.

Метод формирования гипотез. При формировании содержания программы аналитических исследований могут быть выдвинуты предположения о существовании возможных каналов утечки КЗИ в конкретном направлении деятельности организации. Обоснование этого предположения потребует объяснения фактов совершения правонарушений в сфере обращения КЗИ, причин и обстоятельств, обусловивших невыполнение или ненадлежащее выполнение трудовых обязанностей либо гражданско-правовых обязательств. Процесс проверки гипотезы позволит глубже осмыслить объект и предмет изучения и на этой основе сформулировать нетрадиционные варианты решения задачи по обеспечению безопасности организации.

Метод наблюдения в философском понимании представляет собой преднамеренное, планомерное восприятие, осуществляемое с целью выявить существенные свойства и отношения объекта познания. Наблюдатель, в роли которого выступает исследователь, фиксирует вполне определенное поведение работников, занятых в сфере обращения КЗИ. Различают невключенное (сторонний наблюдатель) и включенное (наблюдатель является участником трудового коллектива либо коммерческой сделки) наблюдение. Метод наблюдения предполагает не только сбор информации о явлениях в сфере обращения КЗИ, но и объяснение событий. Применение метода наблюдения позволяет получить исходные эмпирические данные для разработки теоретических положений и рекомендаций по совершенствованию комплексной системы защиты информации в организациях.

Метод сравнительного правоведения базируется на изучении и использовании правового регулирования сходных отношений. Теоретические обобщения исследования основаны на сравнении различия и сходства предметов, относящихся к изучаемому объекту в системе частного права. Сравнение правовых норм носит всегда в правовой системе конкретно-исторический характер, что может быть использовано при характеристике элементов комплексной системы защиты информации в организации. Применение этого метода позволяет получить характеристику сходства и различия сравниваемых отдельных элементов изучаемого объекта в рамках корпоративных, трудовых и гражданско-правовых отношений в сфере обращения КЗИ и охраны ее конфиденциальности .

Метод аналогии исходит из философского принципа, что новое может быть понято через образы старого. Осмысление процес са охраны конфиденциальности информации в современный период основывается на определении его сходства с защитой государственных секретов в советское время по конкретным однопорядковым признакам при соблюдении конкретно-исто рического подхода.

Применение *метода анализа и синтеза* имеет определяющее значение для раскрытия сущности и основных форм развития изучаемого объекта в гражданском (торговом) обороте информации, для группировки проблем, подлежащих изучению, по их значению и взаимосвязям, систематизации их по признакам типологизации. Источником познания явлений, происходящих при обращении КЗИ, служат накопленные определенные знания и практика правового, организационного и методического обеспечения безопасности организаций. Отсюда вытекает определение сущности анализа и синтеза как приемов мышления, состоящих в комплексном, органически взаимо связанном изучении фактов, событий и явлений, связанных с проблемами охраны конфиденциальности КЗИ; выявлении ВКУ КЗИ, причин и обстоятельств, способствующих утечке такой информации, и мерах по их предупреждению. Анализ и синтез могут быть представлены и как вид практической деятельности организации, связанный с необходимостью обеспечения работы юридического департамента и службы безопасности, и поэтому являются основной частью аналитической работы

Применение *метода эксперимента*, выполняющего важную прогностическую функцию, важно тогда, когда: *во-первых,* целесообразность и эффективность того или иного режимного мероприятия, связанного с прогнозированием, нельзя обосновать с помощью иных методов; *во-вторых,* невозможно научно предсказать какие-либо конкретные результаты решения прогнозируемых проблем в сфере обеспечения безопасности организации, так как научное предвидение объясняет, как правило, лишь общие направления и характер этих результатов.

Эксперимент позволяет подтвердить выдвинутую гипотезу и служит источником фактического материала, дает возможность перейти от гипотезы к теории, а от теории — к практике, к выработке научно обоснованных рекомендаций по предупреждению утечки КЗИ. Эксперимент выступает, с одной стороны, как способ проверки, например, установленного в организации режима коммерческой тайны, а с другой — как инструмент, способствующий поиску новых правовых средств, направленных на обеспечение эффективности деятельности по охране конфиденциальности КЗИ.

Математические методы широко используются при исследовании социальных явлений. Математические формулы выражают не только количественные отношения действительности, но и улавливают качественную сторону объекта изучения. Математические методы могут быть использованы при разработке методик определения степени конфиденциальности информации, выявления ВКУ информации и изучения системы предупреждения нарушений в сфере обращения КЗИ, а также для обоснования расчетов, подтверждения тенденции развития того или иного явления. Математический аппарат может быть использован при проведении расчета данных о вероятности возникновения угроз организации, моделирования ВКУ КЗИ и решения других задач в рамках создания АСУРО работ, выполняемых в организации с использованием КЗИ.

Данные *кибернетики* как науки, исследующей различные системы живой природы и автоматические системы, созданные человеком, а также изучающей законы управления в любых системах, в том числе и социальных, могут быть использованы организациями для разработки комплексных систем защиты ин формации. Перспективной в этом направлении является задача изучения возможностей использования кибернетических методов при выявлении угроз безопасности организации, планировании мер по охране КЗИ.

Частнонаучные методы позволяют получить данные о регулировании и обеспечении охраны конфиденциальности информации в гражданском (торговом) обороте с использованием различных правовых средств.

Письменный и устный опрос достаточно часто используется для сбора эмпирических материалов. Опрос как выборочный метод сбора социально-правовой информации в сфере обращения КЗИ может проводиться в виде *анкетирования,* представляющего со бой сбор сведений об имеющихся недостатках в работе, которые связаны с корпоративным регулированием обращения КЗИ, фор мированием договорных условий об охране конфиденциальности информации, принятием адекватных мер угрозам безопасности организации, а также мер по предупреждению нарушений в этой сфере. На практике используются различные формы сбора сведений, в основном в виде устного опроса и заполнения анкет.

Анализ документов — один из широко используемых и эффективных методов, который применяется для сбора первичной информации о состоянии дел в сфере обращения КЗИ и охраны ее конфиденциальности. Документы анализируются на традиционных (бумажных) носителях и электронных документах. Это могут быть официальные и неофициальные, статистические и другие документы в зависимости от возможности доступа к ним, их целостности и легитимности

Метод экспертных оценок позволяет учесть мнение специалистов по определенному кругу вопросов. Экспертами являются руководители организаций и подразделений, научные и практические работники, хорошо знающие исследуемую проблему в области обеспечения безопасности коммерческих структур. Экспертам могут быть заданы следующие вопросы: каково состояние охраны коммерческой тайны в организации; какова величина латентности (т.е. нераскрытых, неизвестных администрации нарушений) в сфере обращения КЗИ, на каких направлениях деятельности организации могут существовать ВКУ КЗИ; каковы причины и условия, спо собствующие совершению нарушений в этой сфере; какие меры следует предпринять для закрытия ВКУ КЗИ и др. Информация, полученная от экспертов, в основном носит не эмпирический, а концептуальный характер и является по этой причине менее детализированной.